

WJN

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Pennsylvania

In the Matter of the Search of  
 (Briefly describe the property to be searched  
 or identify the person by name and address)  
 the former office of Curtis Anderson, Kappa Alpha Psi  
 International Headquarters, 2322 North Broad Street, 2nd  
 floor, Philadelphia PA 19132

Case No. 19- 94 M

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated here by reference

located in the Eastern District of Pennsylvania, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, incorporated here by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

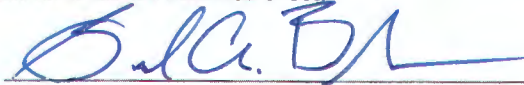
The search is related to a violation of:

Code Section	Offense Description
18 United States Code Sections 1343 and 1344	wire fraud, bank fraud

The application is based on these facts:  
 See attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Samuel A. Bracken, United States Postal Inspector

Printed name and title

Sworn to before me and signed in my presence.

Date: 01/17/2019



Judge's signature

City and state: Philadelphia PA

Timothy R. Rice, United States Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, SAMUEL A. BRACKEN, United States Postal Inspector, United States Postal Inspection Service, being duly sworn, depose and state as follows:

1. I am a United States Postal Inspector assigned to the Philadelphia Division of the United States Postal Inspection Service (“Inspection Service”), and have been so employed since February 2004. I am currently assigned to the Miscellaneous Crimes Team, which investigates violations of federal law including identity fraud, aggravated identity theft, mail fraud, wire fraud and bank fraud, in violation of Title 18, United States Code, Sections 1028(a), 1028A, 1341, 1343 and 1344, respectively. I have received training in investigating identity theft, credit card fraud, wire fraud, bank fraud, and mail fraud offenses, including attending seminars and conferences hosted by the International Association of Financial Crimes Investigators. During my employment as a Postal Inspector, I have participated in hundreds of investigations involving identity fraud, theft of mail, aggravated identity theft, mail fraud, wire fraud and bank fraud. In addition, I have been the Inspection Service’s case agent on numerous investigations involving these offenses.

**PURPOSE OF AFFIDAVIT**

2. This affidavit is submitted in support of an application for a search warrant to search Curtis Anderson’s former work office, located at the Kappa Alpha Psi fraternity, 2322 N. Broad Street, 2<sup>nd</sup> Floor, Philadelphia, PA 19132 (“the fraternity office”).
3. The Inspection Service, the Federal Bureau of Investigation (FBI), the United States Secret Service (USSS), and the Federal Deposit Insurance Corporation – Office of Inspector General (FDIC-OIG) are assisting a federal grand jury that is investigating

Curtis Anderson, the former Director of Finance of the Kappa Alpha Psi fraternity, who is suspected of embezzling an amount in excess of \$1 million from his former employer by means of a scheme involving unauthorized checks and interstate wire transmissions.

4. The facts in this affidavit come from my review of documents, personal observations, information obtained from other agents and witnesses and my training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.
5. Based upon the information set forth in this affidavit, there is probable cause to believe that the fraternity office, more fully described in Attachment A, contains certain items, described in Attachment B, which represent fruits, instrumentalities, and evidence of violations of Title 18, United States Code, Sections 1343 (wire fraud) and 1344 (bank fraud).

#### **DETAILS OF INVESTIGATION**

##### **SANTANDER BANK**

6. In December 2018, the Inspection Service, along with agents from the FBI, USSS, and FDIC-OIG, began an investigation of Curtis Anderson. At that time, Anderson was the Director of Finance for the Kappa Alpha Psi fraternity. Agents received information from Santander Bank, the bank which held accounts for the Kappa Alpha Psi fraternity, that Anderson was cashing checks from the fraternity's checking account, including checks made payable to him and checks made payable to other individuals, as well as conducting direct cash withdrawals from the fraternity's accounts.
7. Santander Bank reported that from March 20, 2018 through October 26, 2018, approximately 87 checks were cashed against the fraternity's accounts with Santander



Bank totaling \$189,539.21. Santander Bank reported that these checks were made payable to either Curtis Anderson, or other third parties, including persons who will be referred to here by their initials: W.W., D.S., N.H., K.H., and G.D., and all were cashed by Anderson at five different Santander Bank locations in Pennsylvania, including branches in Philadelphia, PA and Marcus Hook, PA, all located in the Eastern District of Pennsylvania.

8. Santander Bank reported that with regard to the checks made payable to third parties, Curtis Anderson was the individual cashing the checks. According to Santander Bank, Anderson told Santander representatives when he cashed the checks that the third parties were employees of the fraternity and that he, Anderson, was saving the individuals a trip to the bank by cashing the checks for them.
9. In conjunction with the cashing of the fraternity's checks by Anderson, Santander Bank further reported large deposits into personal bank accounts of Anderson held at Santander Bank. Santander Bank reported that from April 13, 2018 through October 12, 2018, two accounts held solely by Anderson, and a third account, held in joint name by Anderson and his wife, received approximately 65 cash deposits totaling approximately \$101,030.56. In some instances, the deposits into Anderson's account coincided with the cashing of the fraternity's checks. For instance, on May 24, 2018, Anderson cashed a \$2,489.51 check drawn on the fraternity's account and made a \$2,489.51 cash deposit into one of his personal accounts. Another example occurred on October 12, 2018, when Anderson cashed a \$2,342.61 check drawn on the fraternity's account and made a \$2,302.61 cash deposit into one of his personal accounts.

**CONTACT WITH KAPPA ALPHA PSI**

10. On January 14, 2019, FBI Special Agent (SA) Annette Murphy and FDIC-OIG SA Frank Coppola interviewed John Burrell, the executive director of Kappa Alpha Psi, regarding Curtis Anderson's activity. In his interview, Burrell stated that Anderson had been employed by Kappa Alpha Psi since 1986 and had held the title of Director of Finance for the last 20 years. Burrell stated that, as Director of Finance, Anderson had the authority to make deposits into Kappa Alpha Psi accounts, but did not have had any authority to sign checks.
11. Burrell stated that on or about December 19, 2018, he had been contacted by a Santander Bank representative regarding suspicious activity on the Kappa Alpha Psi accounts. Burrell went to meet with the Santander Bank representative that same day to review the suspicious activity.
12. Burrell advised that on December 21, 2018, he again went to Santander Bank to meet with a representative of the bank regarding the suspicious activity. On this date, Burrell was accompanied by Thomas Battles, the National President of Kappa Alpha Psi. Burrell stated that while Burrell and Battles were at Santander Bank that day, they began changing the account access for the fraternity's accounts. Burrell stated further that while he and Battles were at Santander Bank on December 21, Curtis Anderson walked into that same Santander Bank branch. Burrell reported that upon seeing Burrell and Battles, Anderson turned around and left the bank without doing any business. Burrell stated that Battles then called Anderson on his cellular telephone and requested that Anderson return to the Santander Bank branch that he just left.
13. Burrell advised that Anderson returned to the Santander Bank branch, at which time Battles and Burrell showed Anderson copies of the cashed checks from the fraternity's

account that were payable to Anderson. Burrell stated that Anderson then confessed that he had cashed those checks from the fraternity's accounts. Burrell stated that Anderson explained to Burrell and Battles that he had a gambling and drinking problem and that he had spent most of the money at Harrah's Casino.

14. Burrell stated that Anderson last accessed his office at Kappa Alpha Psi when the fraternity allowed Anderson to retrieve his briefcase from that office on December 21, 2018. On December 24, 2018, Anderson was formally fired from Kappa Alpha Psi.
15. Burrell advised that a review of bank accounts held by Kappa Alpha Psi revealed that Anderson had stolen approximately \$400,000 from the fraternity's accounts at Santander Bank and approximately \$978,000 from the fraternity's accounts at Wells Fargo Bank.
16. On January 15, 2019, FDIC-OIG SA Coppola and USSS SA Michael Gannon responded to the office of Kappa Alpha Psi located at 2322 N. Broad Street, Philadelphia, PA 19132 to retrieve documents related to the investigation of Anderson from a representative of the fraternity. While at the offices of Kappa Alpha Psi, agents met with Linwood Green, the interim Director of Finance of Kappa Alpha Psi. Green voluntarily escorted SAs Coppola and Gannon to Anderson's office. SAs Coppola and Gannon saw numerous reams of check paper, a computer, and various signature stamps of Kappa Alpha Psi's signatories. Green told SAs Coppola and SA Gannon that there was no legitimate reason for Anderson to have had the large amount of check stock paper present in his office. Green said that Anderson probably should have not have had any, but if he did, one ream would be the most he would have needed to have in his possession.



17. Green also told SAs Coppola and Gannon that any check written on the fraternity's accounts was supposed to be signed by two fraternity officials: the Executive Director and the Grand Keeper of the Exchequer.
18. SAs Coppola and Gannon learned that Anderson's office is located on the second floor. The offices do not have room numbers. SA Coppola observed that the second floor had four offices in total, with two each on opposite sides of the building, and a copy center.
19. Prior to leaving the offices of Kappa Alpha Psi, SA Coppola requested that no individual access Anderson's office and to keep the door locked. SA Coppola asked that if anyone needed to access the office, to contact him first before they entered.
20. Included in the documents that the fraternity provided on January 15, 2019 to SAs Coppola and Gannon were copies of the checks cashed by Anderson for bank accounts held by the fraternity at Wells Fargo Bank and Santander Bank. These checks appeared to have only one signature on the check, that of Spencer Bruce, a former executive director for the fraternity who is no longer employed there and has not worked at the fraternity since at least May 2018. It is believed that these checks were signed using signature stamps of Bruce. These checks did also not comply with the two signature rule of the fraternity whereby the executive director and Grand Keeper of the Exchequer sign the checks.
21. Further review of the Wells Fargo checks cashed by Anderson show he began cashing the checks on approximately June 1, 2017 and continued through December 18, 2018.

#### **STATEMENT OF EXPERTISE**

22. Based on training and experience your affiant has received regarding financial crimes, your affiant has learned that individuals who commit fraud at their workplace

will often keep documents and other records regarding that fraud in their workplace office, typically for long periods of time. Individual offices, as opposed to common workplace areas, provide spaces where the employee can retain such documents and records, and have them readily available, but also keep such items hidden from the view of co-workers and supervisors.

23. Based on my knowledge, training and experience I know that financial crimes, particularly those involved in this investigation, including embezzlement using checks, committed via wire fraud, are crimes typically committed with the aid of computers and various computer programs, including check-making software. These computers and computer programs can store data related to these unauthorized transactions for months or even years, even if that data has been deleted by the user.
24. Based on my knowledge, training and experience I also know that individuals involved in fraudulent check activity, including forging signatures on documents, will often have on hand various signatures needed to forge signatures, including copies of signatures they have collected or stamps of signatures. These saved signatures can be stamps and signatures on official documents they have collected. They are often saved as hard copies or as computer files, such as .pdf's, .jpg's, or .tif's.
25. Based on my knowledge, training and experience I also know that individuals involved in this kind of fraudulent activity will often keep a ledger or accounting of their fraud, in order to keep track of how much they have stolen from their workplace. This ledger can oftentimes be found on their work computer, usually to keep it hidden from the view of their co-workers, but readily available to them at work.



26. I know that computer hardware, software, documentation, passwords, and data security devices may be important to a criminal investigation in two distinct and important respects: (1) the objects themselves may be instrumentalities, fruits, or evidence of crime, and (2) the objects may have been used to collect and store information about crimes (in the form of electronic data). Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices which are (1) instrumentalities, fruits, or evidence of crime; or (2) storage devices for information about a crime.

27. Based upon the facts set forth above, computer hardware, software, related documentation, passwords, data security devices (as described below), and data located at Curtis Anderson's former office are integral tools of these crimes and constitute the means of committing them. As such, they are instrumentalities and evidence of the violations designated. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them.

a. Hardware

- Computer hardware consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes (but is not limited to) any data processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers); internal and peripheral storage devices (such as fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor type

binary devices, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, and optical readers); and related communications devices (such as modems, cables and connections, recording equipment, RAM and ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

b. Software

- Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like tax preparation, bookkeeping, word-processing, graphics or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

c. Documentation

- Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Passwords and Data Security Devices

- Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security

devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain preset security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

28. Based upon my knowledge, training and experience, and consultations with other law enforcement personnel, I know that searching and seizing information from computers often requires agents to seize most or all electronic storage devices (along with related peripherals, discussed below) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

- a. The volume of evidence
  - Computer storage devices (like hard disks, and diskettes) can store the equivalent of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site, especially at a personal residence.
- b. Technical requirements



- Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password protected, or encrypted files. Because computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment is essential to its complete and accurate analysis.

29. Based upon my knowledge, training and experience, I know that searching computerized information for evidence or instrumentalities of crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true because of the following:

a. The peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software. Many system storage devices require particular input/output (or "I/O") devices in order to read the data on the system. It is important that the analyst be able to properly reconfigure the system as it now operates in order to accurately retrieve the evidence listed above. In

addition, the analyst needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices.

b. If, after inspecting the I/O devices, software, documentation, and data security devices, the analyst determines that these items are no longer necessary to retrieve and preserve the data evidence, the government will return them within a reasonable time.

c. Data analysts may use several different techniques to search electronic data for evidence or instrumentalities of crime. These include, but are not limited to the following: examining file directories and subdirectories for the lists of files they contain; "opening" or reading the first few "pages" of selected files to determine their contents; scanning for deleted or hidden data; and searching for key words or phrases ("string searches").

30. Based on the information received from sources and through investigation, there is reason to believe that Curtis Anderson used computer programs in conjunction with computer hardware, to prepare checks of the fraternity, which play a role in the commission of the offenses described in this affidavit. Therefore, the computer hardware, software, and computer-related documentation used for billing patients or other business purposes at the business constitute means of committing criminal offenses, and are instrumentalities of these criminal violations.

31. I know, through my training and experience, that to properly retrieve and analyze all

electronically stored (computer) data, to insure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, both an on-site analysis and a laboratory analysis by qualified computer specialists will be necessary. Such accuracy and completeness can be achieved only by seizing all computer equipment and peripheral devices which may be interdependent, the software to operate them, and related manuals which contain directions concerning the operation of the computer system and software programs.

32. I know, through my training and experience, that computerized evidence can be subject to loss or destruction following the execution of a search warrant if the evidence is not seized at the time of the search. It is unlikely that the government would be able to obtain the evidence by a follow-up subpoena to the search, because the computer may be re-purposed, to include formatting the memory and then being re-issued to a new user and therefore overwritten. Therefore, it is often necessary to physically remove computers from the locations where they are located. I understand that the removal of computers in cases where they are used for business operations may hinder the daily operation of the business. However, the physical removal may be necessary for the retrieval and protection of the data.
33. The government will make every effort to copy the data described above in electronic format or disk on the date of the search. If it is not technically feasible to copy the data, then the computer software, hardware and data security devices will be removed from the place searched, so that a subsequent search of the computer hardware and software may be accomplished off-premises by personnel designated by the United States Secret Service, who are adequately trained to conduct the search. The original computer



software, hardware and data security devices will be returned immediately after the copying. In the interim, if the fraternity has an ongoing need for data stored on the computers, every attempt will be made to provide the fraternity with any requested information or copies of files.

34. If the computers and digital storage media are physically removed from the business location, every effort will be made to create forensic images of them quickly and to return the computers and digital storage media upon request.

**CONCLUSION**

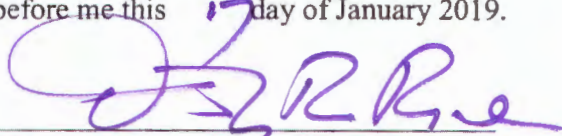
35. Based on my training and experience and the facts set forth in this affidavit, I believe there is probable cause that the items set forth in Attachment B, which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud) and 1344 (bank fraud), are located at the former office of Kappa Alpha Psi Finance Director Curtis Anderson, more fully described in Attachment A.

Based upon the foregoing, I request that the Court issue the proposed search warrant.



SAMUEL A. BRACKEN  
U.S. Postal Inspector  
U.S. Postal Inspection Service

Sworn to and subscribed  
before me this 17 day of January 2019.



TIMOTHY R. RICE  
United States Magistrate Judge